Human element is key to stopping hackers

Informationweek; Manhasset; May 29, 2000; Kelly Jackson Higgins;

Issue:	788
Start Page:	164-173
ISSN:	87506874
Subject Terms:	Hackers Network security Security services
Classification Codes:	**5250**: *Telecommunications systems & Internet communications* **5140**: *Security management* **9190**: *United States*
Geographic Names:	United States US

Abstract:

Intrusion-detection services come with around-the-clock outside experts who collate and sift through all the information, superfluous or not, generated by intrusion-detection sensors sitting on a network. These services manage all the hardware and software tools, too. Companies typically pay a monthly fee for such services. Most security providers package intrusion detection as part of a suite of managed-security offerings that also include firewalls, vulnerability assessment and, in some cases, secure virtual private networks.

Full Text:

[Headnote]

INTRUSION-DETECTION SERVICES PROLIFERATE AS ATTACKS BECOME MORE FREQUENT AND DAMAGING

It was 2 a.m. when the intrusiondetection alarm sounded at DefendNet Solutions Inc. Security technicians at the managed-security services firm scrambled to find the source of the suspicious traffic, which was hitting one of its client's networks. Once they traced it to the source, DefendNet's techs phoned the IT department of the company running the culprit machine. Turns out the unauthorized traffic wasn't a hack attack, but the result of an innocent mistake-a misconfigured Simple Network Management Protocol machine.

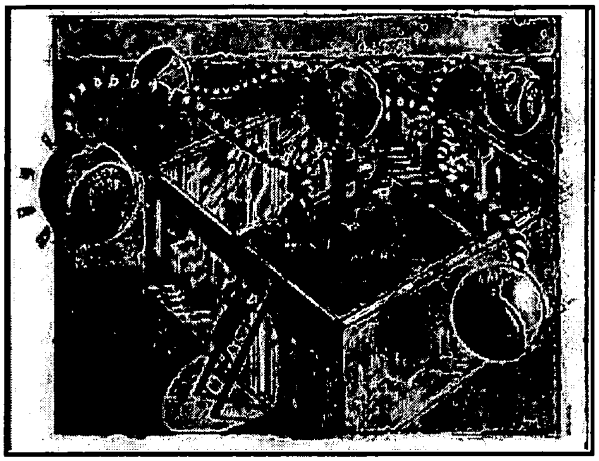
False alarms such as this unfortunately are all too common for intrusiondetection technology. Companies can't rely on the software alone to determine whether, for instance, Internet Message Control Protocol traffic hitting a router is carrying legitimate messages to the device or instead is being used as a vehicle for a denial-of service attack. So the choice is either to have your own security technicians on duty around-the-clock or go with an outsourcing company.

"You really need human interaction to sort and analyze whether an alarm event is significant," says Vincent Giordano, president and CEO of DefendNet.

Intrusion-detection services come with around-the-clock outside experts who collate and sift through all the information, superfluous or not, generated by intrusion-detection sensors sitting on a network. These services manage all the hardware and software tools, too. Companies typically pay a monthly fee for such services.

Most security providers package intrusion detection as part of a suite of managed-security offerings that also include firewalls, vulnerability assessment, and, in some cases, secure virfoal private networks (VPN). Companies such as DefendNet, IBM Global Services, Internet Security Systems (ISS), Pilot Network Services, and RIPTech already offer intrusion-detection services. Other security companies, including Axent Technologies Inc., plan to roll them out soon. The market for managed-security services is expected to reach more than $2 billion worldwide by 2003, up from $512 million in 1998, according to research firm International Data Corp.

Still, intrusion detection is in its infancy. It wasn't long ago that intrusion detection meant paying so-called `white hat" hackers to simulate breakins to a company's network and search for clues of any real attempts. Companies now are under pressure to place full-time monitoring tools at the hot spots in their networks to continuously sniff out and deter intruders.



An intrusion-detection tool works much like an antivirus package. Sensors look for known "signatures," or potential hacker tools and footprints, and notify the main intrusion-detection server if it finds any The server then sends out an alarm. Depending on the security tool or service, the sensor records all these events locally in a log, which can be plucked by the server into a relational database to track trends and generate reports. ISS's ePatrol Managed Intrusion Detection service, for instance, stores information on events in a Microsoft Access and SQL relational database. A tool or service can also be customized to automatically shut down a particularly sensitive port if it receives unauthorized traffic.

With more hackers, crackers, and script kiddies attempting to punch holes in firewalls and plant nefarious codes in the pores of operating systems, it's no longer enough to plop down a firewall at the edge of a network. There are four times as many hacker attacks a day in North America as there were just one year ago, according to ICSA, a security consulting firm.

And the attacks are getting more high-profile and widespread: The distributed denial-of service attacks on sites such as Amazon.com, CNN, and Yahoo in February boosted awareness-and business-for intrusiondetection technology, which basically acts as a burglar alarm on the network.

Security experts predict that the next round of hacker attacks will be more deadly, potentially taking down significant chunks of the Internet by exploiting domain name system servers and Hypertext Markup Language and JavaScript codes to do their dirty deeds.

Some tools and services, such as IBM Global Services', focus only on intrusions at the network level, rather than inside the operating system. But the trend is toward a hybrid networkand host-based solution, such as ISS's ePatrol service. That way, potential problems such as known holes in operating systems as well as the internal corporate security threats are covered by the intrusion tools. "A combination of network- and host-based intrusion detection is critical," says George Kurtz, CEO of Foundstone Inc., a security consulting firm. "If you just do one or the other, you're missing half of the events."

The main differences between managing your own intrusion detection and hiring an outsourcing company are manpower and expertise. When intrusion detection is handled in-house, the alarms can be overwhelming. "When an alarm sounds, no one knows what to do with it," says Bruce Schneier, founder of Counterpane Internet Security Inc., an intrusion-detection company that operates similar to the homesecurity system model.

Schneier says the advantage of a service provider acting as a security guard is that it can analyze all the traffic that gets logged on the intrusion-detection devices-something many enterprise IT departments just don't have the time or resources to do. "The servers, routers, and firewalls log millions of lines of audit logs a day-among all of this are the footprints of an attack," he says. "We're the ones who look through those audit logs and figure out if an event is real."

For startups such as iApex Inc.-an application service provider in Alamo, Calif, that handles transactions for online buyers and sellers-the answer is outsourcing everything, including the network, Web servers, and security technology. The ASP uses Pilot Network Services' VPN service, which comes with intrusion detection built in. "We don't have an infrastructure-Pilot hosts it," says Aran Shrestha, CEO and founder of iApex. "We didn't want to do security on our own. Our strength isn't in keeping up with hacker techniques," he adds.

KNOW YOUR STRENGTHS: Startup iAp chose to outsource everything ft could, including intrusiondetection services, CEO and founder Shrestha says. "We didn't want to do security on our own."

The company pays Pilot about $2,000 per month for the VPN service, in addition to a per-server charge. Building a secured network would have cost the company more than $1 million, says Shrestha.

Still, many businesses that run intrusion-detection tools typically do a combination of in-house and outsourced security. Take the Depository Trust Co. in New York, which uses IBM Global Services to handle intrusion detection at the entry points of its network, and Axent's NetProwler detection tools for watching the inside of the network.

"The risk is high enough, .so why not have a second pair of eyes?" says Stash Jarocki, chief information security officer at Depository Trust. The financial-services firm also subscribes to Global Integrity's Web integrity service, which helps ensure that its site isn't defaced by a graffitihappy hacker.

IBM Global Services uses a different intrusion-detection tool, Cisco's NetRanger, but the different data formats between NetRanger and NetProwler are a nonissue since IBM sends final reports to Depository Trust. And Jarocki says Depository Trust built its own SQL database for correlating data gathered by Axent's Enterprise Security Monitor, NetProwler, and other packages.

Jarocki says he may bring more of the intrusion work in-house, although he hasn't ruled out outsourcing. Another outsourcing arrangement may depend on whether the potential provider lets him pick his own intrusion-detection tool, rather than being forced to go with a vendor solution. "I still want to be able to pick my own intrusion-detection product," Jarocki says. "I don't want to just use the one they provide."

But staffing can be a problem for businesses that want to keep intrusion detection in-house. The IT labor shortage has been especially painful in the security market. "There's a shortage of experts in intrusion detection, and they don't want to work 24-by-7. That's one of the things that drove me to outsourcing intrusion detection," says Kurt Ziegler, chairman and CEO of eBSure, an ASP that does performance monitoring for Web sites. The company uses RIPTech's eSentry service for running its firewalls and intrusiondetection system.

The shortage of expertise is equally tough for intrusion-detection service providers. Every three to five months, RIPTech rotates its security technicians from the monotony of monitoring client networks to doing incident response testing, security audits, and testing. The idea is to keep them refreshed and challenged so they don't burn out on the graveyard shift.

Whatever the approach, there's no such thing as bulletproof security. Even if a company goes with an intrusion-detection service provider, there are no guarantees its security tools and experts will catch every unauthorized ping or Trojan horse. Intrusiondetection tools can't actually stop a denial-of service attack, but they can at least give a heads up if one is infiltrating a network.

"Intrusion detection shouldn't provide a false sense of security," Foundstone's Kurtz says. "There are still many attacks and events that aren't captured, as well as the superfluous information."

NOT ONE ANSWER: Even with an intrusion-detection service, there's still the possibility of hackers shutting down the sensors to sneak into a network depository, Depository Trust's Jarocki says.

And as with antivirus software, network managers have to keep intrusion tools up-to-date with the latest threats. They can't just install the software and let it go. That's the advantage of going with a security provider, which would be responsible for keeping the software updated. "If you buy it off the shelf, install it, and forget about it, you're going to get infected," says Frank Swift, manager of security operations at Pilot Network Services.

Even with an intrusion-detection service, there's the risk of hackers shutting down the sensors so they can sneak into a network, says Depository Trust's Jarocki. That's why risk management and regular audits by white-hat hackers are crucial. "I still use auditors," Jarocki says. "I need proof that we're doing a good job with intrusion-detection services."

Intrusion-detection software has a long way to go before it's truly automated and intelligent, experts say. An intrusion-detection service must be customized to protect a company's internal applications, such as human-resource tools, so its security software can defend against any attacks on that app. "Our consulting group has to have an option in its service [contract] to write company-specific attack measures," says Scott Gordon, director of product management for Agent Technologies.

An ironic twist is that encryption can block a sensor. Intrusion tools can't read traffic encrypted in a Secure Sockets Layer session. But an intrusion tool or service that includes host-based monitoring would have a chance of detecting an attack once the server on the receiving end decrypts the traffic, Foundstone's Kurtz says.

The next generation of intrusiondetection products and services will be more intelligent and able to make more informed decisions on whether to shut down a port under siege. "Down the road it will be more self learning, with the system being able to pick up trends from signatures of attack," says DefendNet's Giordano.

Even with all the potential automation for these tools, intrusion detection still will require human interaction from a security group, which could include the help desk, the telecommunications staff, and, if it's a big event, the management and legal staffs. Says Depository Trust's Jarocki, "You can never take the human element out of it." -KELLY JACKSON HIGGINS, REPRINTED FROM INTERNETWEEK More on intrusion-detection services: informationweek.com/788/intrusion.htm

[Sidebar]

Providers Offer A Variety Of Intrusion-Detection Services

It's only the beginning. Aside from traditional intrusion-detection companies such as Axent Technologies Inc. and Internet Security Systems Inc. moving to more of an application service provider model, and a raft of newcomers such as Intrusion.com Inc. and DefendNet Solutions Inc., more managedsecurity offerings are on the way About 10 new providers will get funding within a month or so, says Matthew Kovar, a program manager at consulting firm the Yankee Group.

Here are some of the intrusion-detection services available today:

Pilot Network Services Inc. offers an overall secure IP network service with built-in intrusion detection. Pilot's proprietary heuristic Defense Infrastructure technology "learns" from past network events and applies that knowledge when it takes action or does other tracking. HDI runs either automated or semi-automated searching files, checking for known signatures and suspicious traffic, says Phil Simmonds, director of technical marketing at Pilot. The service also relies on Pilot's security technicians, who analyze network traffic.

All three of Pilot's main network services-secure Internet, secure hosting, and virtual private networks--come with intrusion detection. As with any secure IP network service, the catch is that you have to be a Pilot subscriber. Pilot's secure Internet access service, which includes intrusion and other security services, starts at $6,500 a month plus a $13,500 setup fee; its VPN service is priced at $1,000 a month plus a $6,000 setup fee for 400 users.

IBM Global Services has been offering networkintrusion services for three years as part of its consulting, vulnerability, and virus services. Michael Puldy, global solutions executive for IBM, says most of its customers go with the vulnerability/intrusion-detection service combination. He says customers can count on IBM Global Services to review their environments and add intrusion detection if someone is trying to break in.

IBM Global Services has experienced a surge in intrusion business of late, says Puldy, who adds that IBM is in discussions with host-based intrusion providers to possibly expand the service to watching the operating system as well. IBM's service starts at $37,500 a year. The idea is to offer customers suggestions for taking action in response to an event. IBM uses data mining to correlate overall attack trends, which lets it anticipate what might happen next.

Internet Security Systems, one of the top intrusion-software companies, is moving into the services market, thanks to its acquisition last year of managed-security services provider Netrex Secure Solutions. However, Allen Vance, director of offer management for managed security services at ISS, says software still represents about 65% of the company's business; managed services make up about 20%. ISS also touts its relational database support, which includes Microsoft Access. Users can generate reports and store lots of data, but without a full-blown Oracle database, says Vance.

ISS sells the bulk of its software and services through partners such as BellSouth Corp., which offers ISS's ePatrol Managed Intrusion Detection service and other managed security services to its IP customers. ISS next month will add a Unix intrusion-detection appliance to its product repertoire. ISS charges about $3,000 a month for intrusion-detection services and between $1,000 and $3,000 a month for managing a firewall.

DefendNet offers a service for small and midsize companies. For about $200 a month, DefendNet will put a firewall on a company's site and handle all secu= city filtering, host- and network-level intrusiondetection tracking, and reconnaissance. DefendNet typically markets its service through small Internet service providers.

RIPTech Inc.'s Esentry software has its roots in the Department of Defense, where company cofounder and president Amit Yoran helped deploy what was the world's largest intrusion-detection infrastructure. RIPTech's intrusion service is based on a Microsoft SQL relational database with datamining features, and it supports various firewall and intrusion-detection tools. The company's operations center analyzes each event from its sensors. RIPTech remotely manages the security infrastructure and recommends how to respond to events.

Counterpane Internet Security Inc. takes the home-security system approach, acting as a burglar-alarm service. Bruce Schneier, founder of Counterpane, says the company installs sensors on its customers' sites and then waits and responds to alarms. The service provider charges about $12,000 a month. -KELLY JACKSON HIGGINS